

A simple quantum channel having superadditivity of channel capacity

Masahide Sasaki[†], Kentaro Kato^{††}, Masayuki Izutsu[†], and Osamu Hirota^{††}

[†]*Communication Research Laboratory, Ministry of Posts and Telecommunications
Koganei, Tokyo 184, Japan*

^{††}*Research Center for Quantum Communications, Tamagawa University
Tamagawa-gakuen, Machida, Tokyo 194, Japan*

When classical information is sent through a quantum channel of nonorthogonal states, there is a possibility that transmittable classical information exceeds a channel capacity in direct use of the initial channel by extending it into multi-product channel. In this letter, it is shown that this remarkable feature of a quantum channel, so-called superadditivity, appears even in as low as the third extended coding of the simplest binary input channel. A physical implementation of this channel is indicated based on cavity QED techniques.

Superadditivity of the classical information channel capacity is a remarkable feature in quantum communication. Namely, it is expected that more classical information can be sent through a n -product channel than n times the amount that can be sent through a single use of a channel. Let $\{1, \dots, N\}$ be input alphabet with respective prior probabilities $\{\xi_1, \dots, \xi_N\}$, and let $\{\hat{s}_1, \dots, \hat{s}_N\}$ be corresponding input quantum states, called letter states. A decoding is described by the probability operator measure (POM) $\{\hat{\pi}_1, \dots, \hat{\pi}_{N'}\}$ corresponding to output alphabet $\{1, \dots, N'\}$. A quantum channel is a mapping $\{1, \dots, N\} \mapsto \{1, \dots, N'\}$ where quantum noises arise in decoding process itself when at least a pair of $\{\hat{s}_i\}$ is non-commuting which is the case considered here. For fixed $\{\xi_i\}$ and $\{\hat{\pi}_i\}$, the mutual information is defined as

$$I(\xi : \hat{\pi}) = \sum_i \xi_i \sum_j P(j|i) \log_2 \left[\frac{P(j|i)}{\sum_k \xi_k P(j|k)} \right], \quad (0.1)$$

where $P(j|i) = \text{Tr}(\hat{\pi}_j \hat{s}_i)$ is a conditional probability that the alphabet j is chosen when the alphabet i is true. The classical information channel capacity is defined as the maximum value of this mutual information obtained by optimizing $\{\xi_i\}$ and $\{\hat{\pi}_i\}$,

$$C_1 \equiv \max_{\{\xi_i\}, \{\hat{\pi}_j\}} I(\xi : \hat{\pi}). \quad (0.2)$$

In classical information theory, faithful signal transmission is possible by using a certain channel coding if a transmission rate $R = \frac{1}{n} \log_2 M$, where M is a number of codewords and n is a length of the codewords, is kept below C_1 . In contrast, if the quantum noise in the channel is handled properly relying on quantum information theory, the transmission rate R can be raised up to the von Neumann entropy, $H(\hat{\rho})$,

$$H(\hat{\rho}) = -\text{Tr}(\hat{\rho} \log_2 \hat{\rho}), \quad \text{where } \hat{\rho} = \sum_i \xi_i \hat{s}_i. \quad (0.3)$$

So the von Neumann entropy is indeed the quantum channel capacity [1]. This fact has recently been proved by Hausladen et. al. for a pure-state case [2], and has been completed by Holevo including a mixed-state case [3]. It is called the quantum channel coding (QCC) theorem.

A basic channel coding consists of a concatenation of the letter states in a length n and a pruning of all the possible N^n sequences $\{\hat{s}_{i_1} \otimes \dots \otimes \hat{s}_{i_n}\}$ into M codewords $\{\hat{S}_m | m = 1, \dots, M\}$. Assigning an input distribution $\{\zeta_m\}$ to the codewords, the classical capacity for the above kind of n -th extended quantum channel can be defined as

$$C_n \equiv \max_{\{\zeta_m\}, \{\hat{S}_m\}, \{\hat{\Pi}_j\}} I(\zeta, \hat{S} : \hat{\Pi}), \quad (0.4)$$

where $\{\hat{\Pi}_j\}$ is the POM for decoding the codewords. Then, the QCC theorem means $C_n \geq nC_1$, the superadditivity of the classical capacity. By contrast, in classical information theory, the capacity is additive, i.e., $C_n = nC_1$.

It may be plausible that its origin is a quantum correlation among letter states, i.e., an entanglement, generated by a quantum measurement in decoding. However, there has been no guiding principle for utilizing the entanglement correlation so as to produce the superadditivity. Even its direct and unambiguous example, not like an asymptotic one in the length $n \rightarrow \infty$, has not been found yet. A related work was done by Peres and Wootters [4]. They considered

three linearly dependent spin- $\frac{1}{2}$ states $\{|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle\}$ with equal prior probabilities, and studied the amount of the mutual information obtained by several kinds of quantum measurements. They showed that the mutual information obtained by using three 2-bit states $\{|\phi_1\rangle \otimes |\phi_1\rangle, |\phi_2\rangle \otimes |\phi_2\rangle, |\phi_3\rangle \otimes |\phi_3\rangle\}$ and by applying the combined measurement can be larger than twice of the optimum amount attained by using the three initial 1-bit letter states. This must be a gain due to a channel coding. In order to show the superadditivity, however, one must know the C_1 which was not given in their work. In the above kinds of linearly dependent letter states, the C_1 is obtained by setting one of the prior probabilities zero and the others equal, and by applying a standard von Neumann measurement, which is indeed binary quantum channel [5]. Then a comparison between the mutual information of an extended channel and the C_1 does not seem to make sense because this logic leads to a situation that all kinds of sets of more than three linearly dependent letter states may be compared with the C_1 of the binary channel.

An example shown in this letter would be unambiguous and more surprising. This is the simplest case of binary input letter states, $\{|+\rangle, |-\rangle\}$, for which identification of the classical capacity C_1 is established [6,7,8]. In this case, the optimization can be achieved by the binary symmetric channel with the decoding by $\{\hat{\pi}_i = |\omega_i\rangle\langle\omega_i|\}$ where

$$\begin{aligned} |\omega_1\rangle &= \left(\sqrt{\frac{1+c}{2}} + \kappa\sqrt{\frac{1-c}{2(1-\kappa^2)}}\right)|+\rangle - \sqrt{\frac{1-c}{2(1-\kappa^2)}}|-\rangle, \\ |\omega_2\rangle &= \sqrt{\frac{1+c}{2(1-\kappa^2)}}|-\rangle + \left(\sqrt{\frac{1-c}{2}} - \kappa\sqrt{\frac{1+c}{2(1-\kappa^2)}}\right)|+\rangle, \end{aligned}$$

with $\kappa = \langle + | - \rangle$, being assumed to be real, and $c = \sqrt{1 - \kappa^2}$. Then the capacity C_1 is given as

$$C_1 = 1 + (1 - p) \log_2(1 - p) + p \log_2 p, \quad (0.5)$$

where $p = (1 - \sqrt{1 - \kappa^2})/2$.

Now we would like to show that the superadditivity of the classical information channel capacity reveals itself in the third-extended coding. The four sequences $\{|S_i\rangle\} = \{|++\rangle, |+-\rangle, |-+\rangle, |--\rangle\}$ are picked up as the codewords from 8 possible sequences. They can encode 2-bit classical information. We fix here their prior probabilities as 1/4. In decoding, the so-called square-root measurement [2,9,10] is applied. Let $\{|\mu_i\rangle\}$ be the measurement states. Giving the Gram matrix $\hat{\Gamma} = (\langle S_i | S_j \rangle)$, the channel matrix elements are then given as $x_{ij} \equiv \langle \mu_i | S_j \rangle = (\hat{\Gamma}^{\frac{1}{2}})_{ij}$. It is straightforward that

$$\begin{aligned} x_{ii} &= \frac{1}{4}(\sqrt{1 + 3\kappa^2} + 3\sqrt{1 - \kappa^2}), \quad \forall i, \\ x_{ij} &= \frac{1}{4}(\sqrt{1 + 3\kappa^2} - \sqrt{1 - \kappa^2}), \quad i \neq j. \end{aligned} \quad (0.6)$$

Moreover one can confirm that this measurement attains the minimum average error probability, that is, x_{ij} satisfies the Holevo condition [9,11]. The mutual information is simply given as

$$I_3(S : \mu) = 2 + x_{11}^2 \log_2 x_{11}^2 + 3x_{12}^2 \log_2 x_{12}^2. \quad (0.7)$$

Then it can be seen that $I_3(S : \mu)/3 > C_1$ for $0.74 < \kappa < 1$, as shown in Fig. 1 (a) and (b). This ensures the superadditivity $C_3 > 3C_1$. Fig. 1 (c) shows the minimum average error probability $P_e^{(3)}(\text{opt})$. In almost the same region of κ in which $C_3 > 3C_1$ holds, $P_e^{(3)}(\text{opt})$ becomes larger than the minimum average error probability, p , of the initial channel. Thus, while the reliability in terms of the average error rate degrades by the coding, the transmittable classical information can be raised up. This is in sharp contrast to a result from classical information theory that the third extension falls short of correcting even one bit error so that the obtained mutual information is far below C_1 . The other combination $\{|++\rangle, |--\rangle, |+-\rangle, |-+\rangle\}$ does not show the superadditivity (see one-dotted line in Fig. 1). In the second-extended coding, the superadditivity never appears.

Let us consider n -th extension. There are totally 2^{n-1} sequences whose minimum Hamming distance is 2. Suppose all of them are used as codewords with equal input probabilities. Then in similar way to the above, we can calculate an accessible mutual information $I_n(S : \mu)$ by applying the square root measurement giving the Gram matrix. We have confirmed that the region of κ where the superadditivity appears extends from $\kappa = 1$ to lower value as n increases. The numerical results for $n = 5 \sim 13$ are shown in Fig. 2. It is also worth mentioning that if all of the sequences, totally 2^n , are used as the codewords, $\{\hat{s}_{i_1} \otimes \cdots \otimes \hat{s}_{i_n}\}$ with the prior probabilities $\{\xi_{i_1} \times \cdots \times \xi_{i_n}\}$, the optimum decoding is realized by

$$\hat{H}_{i_1 \cdots i_n} = \hat{\pi}_{i_1} \otimes \cdots \otimes \hat{\pi}_{i_n} \quad (0.8)$$

for both the average error probability and the mutual information [12], whose proof will be given elsewhere. In this case, the decoding process generates no entanglement among the letter states, and the resulting capacity is merely

additive. Once the sequences are pruned, a decoding process may include some entanglement correlations. But necessary and sufficient conditions for inducing the superadditivity have not been clear yet.

Now let us move to a realization problem of the above kind of quantum channel, especially, an implementation of the decoding process. So far there has been no explicit physical model corresponding to the quantum optimum decoding of codewords. We model the source $\{|+\rangle, |-\rangle\}$ by superposition states between upper- ($|\uparrow\rangle$) and lower-level ($|\downarrow\rangle$) states of a two-level atom. Namely, a series of atoms is prepared only in $|\uparrow\rangle$ -state, and then it passes through an encoder by which some of the atoms are transferred into $|\nearrow\rangle = \hat{R}_y(\phi)|\uparrow\rangle$ by a rotator

$$\hat{R}_y(\phi) = \begin{pmatrix} \cos\frac{\phi}{2} & \sin\frac{\phi}{2} \\ -\sin\frac{\phi}{2} & \cos\frac{\phi}{2} \end{pmatrix}. \quad (0.9)$$

$\{|\uparrow\rangle, |\nearrow\rangle\}$ are regarded as the letter states $\{|+\rangle, |-\rangle\}$.

We consider n -th extension and let \mathcal{H}_{2^n} be the n -th extended Hilbert space which is spanned by an orthonormal basis states:

$$\begin{aligned} |\uparrow\rangle|\uparrow\rangle\cdots|\uparrow\rangle|\uparrow\rangle &\equiv |A_1\rangle, \\ |\uparrow\rangle|\uparrow\rangle\cdots|\uparrow\rangle|\downarrow\rangle &\equiv |A_2\rangle, \\ &\vdots \\ |\downarrow\rangle|\downarrow\rangle\cdots|\downarrow\rangle|\uparrow\rangle &\equiv |A_{2^{n-1}}\rangle, \\ |\downarrow\rangle|\downarrow\rangle\cdots|\downarrow\rangle|\downarrow\rangle &\equiv |A_{2^n}\rangle. \end{aligned} \quad (0.10)$$

Let $\{|S_1\rangle, \dots, |S_M\rangle\}$ ($M < 2^n$) be the codewords actually used in the channel and $\{|S_{M+1}\rangle, \dots, |S_{2^n}\rangle\}$ be the rest of them. The former set spans the M -dim signal space \mathcal{H}_s . Our concern is an implementation of the square-root measurement described by $\{|\mu_m\rangle|m=1, \dots, M\}$. $\{|S_i\rangle\}$ can be expanded by $\{|A_i\rangle\}$ as,

$$\begin{pmatrix} |S_1\rangle \\ \vdots \\ |S_{2^n}\rangle \end{pmatrix} = \hat{C} \begin{pmatrix} |A_1\rangle \\ \vdots \\ |A_{2^n}\rangle \end{pmatrix}, \quad \hat{C} = (\langle\rho_i|A_j\rangle). \quad (0.11)$$

Since M codewords are linearly independent, $\{|\mu_m\rangle\}$ forms a complete orthonormal set on \mathcal{H}_s . Based on this set, the following orthonormal states can be introduced,

$$|\mu_i\rangle = \frac{|S_i\rangle - \sum_{k=1}^{i-1} |\mu_k\rangle\langle\mu_k|S_i\rangle}{\sqrt{1 - \sum_{k=1}^{i-1} |\langle\mu_k|S_i\rangle|^2}}, \quad (0.12)$$

where $i = M+1, \dots, 2^n$. We denote another expansion by $\{|\mu_i\rangle|i=1, \dots, 2^n\}$ as,

$$\begin{pmatrix} |S_1\rangle \\ \vdots \\ |S_{2^n}\rangle \end{pmatrix} = \hat{B} \begin{pmatrix} |\mu_1\rangle \\ \vdots \\ |\mu_{2^n}\rangle \end{pmatrix}. \quad (0.13)$$

The two basis sets are connected via a unitary operator \hat{V} as,

$$|S_i\rangle = \hat{V}^\dagger |A_i\rangle, \quad (i = 1, \dots, 2^n), \quad (0.14a)$$

where

$$\hat{V}^\dagger = \sum_{i,j} v_{ji} |A_j\rangle\langle A_i|, \quad v_{ji} = (\hat{B}^{-1}\hat{C})_{ij}. \quad (0.14b)$$

The minimum error probability is obtained as

$$P_e(\text{opt}) = 1 - \sum_{m=1}^M \zeta_m |\langle\rho_m|\hat{V}^\dagger|A_m\rangle|^2, \quad (0.15)$$

where $\{\zeta_m\}$ is a priori distribution of the codewords. This means that the decoding by $\{|\mu_m\rangle\}$ can be equivalently achieved first by transforming the codewords $\{|S_m\rangle\}$ by the unitary transformation \hat{V} and then by performing a von Neumann measurement $\{|A_m\rangle\langle A_m|\}$ [13], which is merely a level detection of individual particles (letter states). In this scheme, what brings the entanglement among the letter states is the unitary transformation \hat{V} .

The problem is then an implementation of \hat{V} on the whole space \mathcal{H}_{2^n} . Barenco. et. al. [14] showed that an exact *simulation* of any discrete unitary operator can be carried out by using a quantum computing network. What we require here is not a *simulation* but rather a real *operation* acting on the atomic states constituting the codewords. This can be accomplished by applying a 2-bit gate which works with *target* and *control* bits as a single atomic species. Sleator and Weinfurter have already proposed such a model based on the cavity QED method [15] (the S-W model, henceforth).

At first, \hat{V} is decomposed into $U(2)$ -operators $\hat{T}_{j,i}$ [16] as,

$$\hat{V} = \hat{D}\hat{T}_{2,1}\hat{T}_{3,1}\cdots\hat{T}_{2^n,2^n-2}\hat{T}_{2^n,2^n-1}, \quad (0.16a)$$

where

$$\hat{T}_{j,i} = \exp[-\gamma_{ji}(|A_i\rangle\langle A_j| - |A_j\rangle\langle A_i|)]. \quad (0.16b)$$

($\langle\uparrow|\downarrow\rangle$ is assumed to be real.) Then the above 2-dim rotations are converted into networks of 2-bit gates by using the formula established by Barenco et. al. [14]. We are especially concerned with the case of $n = 3$ in which the superadditivity can appear. For this case, the principle of the formula can easily be understood by showing an example, say, a rotation $\exp[-\gamma(|\uparrow\uparrow\uparrow\rangle\langle\downarrow\uparrow\downarrow| - |\downarrow\uparrow\downarrow\rangle\langle\uparrow\uparrow\uparrow|)]$. It can be executed by the following network,

Diagram 1.

All the notations are borrowed from ref. [14]. The block denoted as \hat{M} is for mapping $\{|\uparrow\uparrow\uparrow\rangle, |\downarrow\uparrow\downarrow\rangle\}$ into $\{|\downarrow\uparrow\uparrow\rangle, |\downarrow\downarrow\downarrow\rangle\}$. In the mapped plane, the desired rotation is carried out as the 3-bit gate operation $\bigwedge_2(\hat{R}_y(2\gamma))$. The two 3-bit gates in the above diagram can be further decomposed into networks consisting of the 1-bit gates, $\bigwedge_0(\hat{R}_y(\pm\gamma))$ and $\bigwedge_0(\sigma_x)$, and the 2-bit gate $\bigwedge_1(\sqrt{\sigma_x})$ [14]. Implementations of the 1-bit gates are straightforward by using the Ramsey zone (RZ) described by the following unitary operator:

$$\hat{U}_R(\tau, |\epsilon\rangle) = \begin{pmatrix} e^{-i\nu\tau/2}\cos(|\epsilon|\tau) & e^{-i\nu\tau/2}\sin(|\epsilon|\tau) \\ -e^{i\nu\tau/2}\sin(|\epsilon|\tau) & e^{i\nu\tau/2}\cos(|\epsilon|\tau) \end{pmatrix}, \quad (0.17)$$

where ϵ is a complex amplitude of a pumping field, the angular frequency ν corresponds to an atomic level separation, and τ is an interaction period.

The required 2-bit gate can be effected by the S-W model which is modeled by the Jaynes-Cummings Hamiltonian,

$$\begin{aligned} \hat{H} = & \hbar\omega\hat{a}^\dagger\hat{a} + \frac{1}{2}\hbar\nu(|\uparrow\rangle\langle\uparrow| - |\downarrow\rangle\langle\downarrow|) \\ & + \hbar g(\hat{a}^\dagger|\downarrow\rangle\langle\uparrow| + \hat{a}|\uparrow\rangle\langle\downarrow|), \end{aligned} \quad (0.18)$$

where \hat{a} (\hat{a}^\dagger) is an annihilation (creation) operator for a cavity field with an angular frequency ω , g is a coupling constant between the cavity field and the atom. It is assumed that ν is originally detuned from the cavity resonant frequency ω so that the atom undergoes an off-resonant interaction whose time evolution is given in the spinor representation as,

$$\hat{U}_{\text{off}}(t) = \sum_{n=0}^{\infty} |n\rangle\langle n| \begin{pmatrix} e^{-i(\frac{\nu}{2} + g_{\text{eff}})t - i n g_{\text{eff}} t} & 0 \\ 0 & e^{\frac{i\nu t}{2} + i n g_{\text{eff}} t} \end{pmatrix}, \quad (0.19)$$

where $g_{\text{eff}} = g^2/\delta$, $\delta = \nu - \omega$, and $|n\rangle$ is n -photon state. Phase factors involving ω have been omitted since it will give no physical effect. If ν is tuned to ω by an appropriate Stark shifting, an on-resonant interaction can be carried out as,

$$\hat{U}_{\text{on}} = \begin{pmatrix} 0 & -i|0\rangle\langle 1| \\ -i|1\rangle\langle 0| & |0\rangle\langle 0| \end{pmatrix}, \quad (0.20)$$

where the interaction period t_0 is chosen as $gt_0 = \frac{\pi}{2}$ and the fact is taken into account that the cavity field is either $|0\rangle$ or $|1\rangle$ throughout the gate operation. Denoting the control-, target-bit atoms and the cavity as “a”, “b” and “c”, respectively, $\Lambda_1(\sqrt{\sigma_x})$ can be realized by applying a unitary process,

$$\hat{R}_z^{(a)}(-\frac{5}{4}\pi) \hat{R}_x^{(a)}(\pi) \hat{U}_{\text{on}}^{(a,c)} \hat{U}_R^{(b)}(\tau', |\epsilon'|) \\ \cdot \hat{U}_{\text{off}}^{(b,c)}(t) \hat{U}_R^{(b)}(\tau, |\epsilon|) \hat{U}_{\text{on}}^{(a,c)} \hat{R}_x^{(a)}(\pi)$$

where the superscript indicates on what system(s) the operator acts. Here $|\epsilon|\tau = |\epsilon'|\tau' = \frac{\pi}{4}$ and

$$i\frac{\nu(\tau - \tau')}{2} - i\frac{\nu t}{2} - i\frac{g_{\text{eff}} t}{2} = 2\pi n \quad (n = \text{integer}),$$

should be satisfied.

In summary, we have proposed a physical model of a quantum channel showing the superadditivity of the classical information channel capacity. It consists of four 3-bit codewords as input signals and the quantum optimum detection which can be realized as a quantum gate network based on cavity QED technique.

The authors would like to thank Prof. A. S. Holevo of Steklov Mathematical Institute, Dr. M. Ban of Hitachi Advanced Research Laboratory, Dr. K. Yamazaki and Dr. M. Osaki of Tamagawa University, Tokyo, for their helpful discussions.

- [1] A. S. Holevo, Probl. Peredachi Inform. vol 15, no. 4, 3 (1979).
- [2] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland and W. K. Wootters, Phys. Rev. **A54**, 1869 (1996).
- [3] A. S. Holevo, Report No. quant-ph/9611023, Nov. (1996).
- [4] A. Peres and W. K. Wootters, Phys. Rev. Lett. **66**, 1119 (1991).
- [5] M. Osaki and O. Hirota (private communication).
- [6] C. A. Fuchs and A. Peres, Phys. Rev. **A53**, 2038 (1996).
- [7] M. Ban, K. Yamazaki, and O. Hirota, Phys. Rev. **A55**, 22 (1997).
- [8] M. Osaki, M. Ban, and O. Hirota (unpublished).
- [9] C. W. Helstrom : *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
- [10] A. S. Holevo, Theory Prob. Appl., vol. 23, 411, June(1978).
- [11] A. S. Holevo, J. Multivar. Anal. **3**, 337, (1973).
- [12] Concerning to the optimality of the mutual information, the authors are indebted to the private communication from A. S. Holevo.
- [13] M. Sasaki and O. Hirota: Phys. Lett. **A210**, 21 (1996); *ibid* **A224**, 213 (1997); M. Sasaki, T. S. Usuda, and O. Hirota, A. S. Holevo, Phys. Rev. **A53**, 1273, (1996); M. Sasaki and O. Hirota, *ibid* **54**, 2728, (1996).
- [14] A. Barenco, C. H. Bennet, R. Cleve, D. P. M. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. **A52**, 3457, (1995).
- [15] T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).
- [16] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).

FIG. 1. (a) The mutual information and the C_1 as a function of κ . The solid line represents the mutual information per bit of the channel consisting of input codewords $\{| + ++ \rangle, | + -- \rangle, | - ++ \rangle, | - +- \rangle\}$ with equal prior probabilities and the square-root measurement for them. The one-dotted line corresponds to the case of the other input codewords $\{| + ++ \rangle, | - ++ \rangle, | + -- \rangle, | - -- \rangle\}$. The C_1 (dashed line) is attained by the binary symmetric channel explained in the text. (b) Same as (a), but for the region $0.7 < \kappa < 1$. (c) The minimum average error probabilities corresponding to the three kinds of channels in (a), as a function of κ .

FIG. 2. The difference between mutual information per symble and the C_1 as a function of κ for $n = 5 \sim 13$. The region of κ where the superadditivity appears becomes wider.